IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

CASSONDRA JOSEPH, individually and on behalf of other similarly situated persons, Plaintiff, v. SAKS INCORPORATED; LORD & TAYLOR LLC; and HUDSON'S BAY COMPANY, Defendants	Case No.: _____ **CLASS ACTION COMPLAINT** **Jury Demand**

KAPLAN FOX & KILSHEIMER LLP
David A. Straite
Ralph E. Labaton
850 Third Avenue
New York, NY 10022
dstraite@kaplanfox.com
Tel.: 212.687.1980
Fax: 212.687.7714

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King
350 Sansome Street
Suite 400
San Francisco, CA 94104
lking@kaplanfox.com
Tel: 415.772.4700
Fax: 415.772.4707

I. INTRODUCTION

1. This is a consumer data privacy class action seeking money damages and injunctive relief on behalf of Plaintiff Cassondra Joseph ("Plaintiff") and other similarly situated customers domiciled in the United States who used their credit cards and other payment cards to make in-store purchases at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor stores (the "Class Members") between May 1, 2017 and the present (the proposed "Class Period").

2. Plaintiff brings this class action case against Saks Incorporated ("Saks"), Lord & Taylor LLC ("L&T"), and their parent company Hudson's Bay Company ("HBC" or the "Company") (collectively "Defendants") for their failure to secure and safeguard consumers' personally identifiable information ("PII") which Defendants collected from various sources in connection with the operation of the Saks and L&T branded subsidiaries.

3. On April 1, 2018, HBC issued a press release (the "April 1, 2018, Press Release") stating that its customers' PII—mainly consisting of credit card numbers linked to actual customer names—had been stolen (the "Data Breach"). Specifically, HBC stated the following:

> HBC Provides Information about Data Security Issue in Certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor Stores in North America
>
> April 01, 2018 11:50 AM Eastern Daylight Time NEW YORK & TORONTO--(BUSINESS WIRE)—HBC (TSX:HBC) today announced that it has become aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. While the investigation is ongoing, there is no indication at this time that this affects the Company's e-commerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe.
>
> The Company deeply regrets any inconvenience or concern this may cause. HBC wanted to reach out to customers quickly to assure them that they will not be liable for fraudulent charges that may result from this matter. HBC has identified the issue, and has taken steps to contain it. Once the Company has more clarity around the facts, it will notify customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. HBC

> encourages customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.
>
> The Company is working rapidly with leading data security investigators to get customers the information they need, and the investigation is ongoing. HBC is also coordinating with law enforcement authorities and the payment card companies.
>
> For further information, please visit https://www.saksfifthavenue.com/securityinformation/notice.html,https://www.saksoff5th.com/securityinformation/notice.html, or https://www.lordandtaylor.com/securityinformation/ notice.html.
>
> In the coming days, customer care representatives will be available through a dedicated call center to provide further information. The call center information will be posted on the above websites at that time.

4. Plaintiff's and other class members' PII was compromised because of Defendants' failure to properly protect the data and falsely represented that the data would be protected.

5. Defendants could have and should have prevented the Data Breach. Defendants chose instead to disregard their data protection duties by (1) failing to take reasonable and adequate measures to ensure secure data systems, (2) failing to disclose to customers that it did not have or maintain adequate computer systems and security practices, (3) failing to take available steps to prevent the Data Breach from occurring, and (4) failing to monitor and detect the Data Breach in a timely fashion.

6. Due to the Data Breach, Plaintiff's and other Class Members' PII is available for criminals' misuse – and the presence of the data on the Dark Web has been confirmed by researchers. Plaintiff and the Class suffered or are likely to suffer injury as a direct result of the Data Breach.

7. Plaintiff also retains a significant interest in ensuring that her PII maintained by Defendants is protected from additional breaches.

8. Plaintiff's and the Class' injuries were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for PII.

9. Plaintiff seeks the following remedies, among others: (1) statutory damages under state law, (2) reimbursement of out-of-pocket losses, (3) other compensatory damages, (4) robust credit monitoring services with accompanying identity theft insurance, and (5) injunctive relief, including an order requiring Defendants to implement improved data security measures.

II. JURISDICTION AND VENUE

10. Plaintiff is a citizen and resident of the State of New York, and asserts claims on behalf of citizens of all fifty States.

11. Defendant Hudson's Bay Company is a Canadian corporation amalgamated under the Canada Business Corporations Act and domiciled in Canada.

12. Defendant Saks Incorporated is a Tennessee corporation headquartered in New York, New York, and is therefore a citizen of Tennessee and New York.

13. Defendant Lord & Taylor LLC ("L&T") is a Delaware limited liability company headquartered in New York, New York. It is a sole member LLC owned by HBC. Pursuant to 28 U.S.C. § 1332, Saks is deemed to be either (a) a citizen of Canada,[1] or (b) a citizen of

[1] The Second Circuit has not yet taken a position on whether the citizenship of a limited liability company is determined by 28 U.S.C. § 1332(d)(10). *See Carter v. HealthPort Technologies, LLC*, 822 F.3d 47, 59-60 (2d Cir. 2016). In this case, regardless of whether section 1332(d)(10) applies to LLCs, this Court nevertheless has CAFA jurisdiction because of the citizenship of HBC and the Plaintiff, and because the proposed class includes members from states other than Massachusetts, New York, and Delaware.

Delaware and New York, if an LLC is deemed to be an "unincorporated association" pursuant to 28 U.S.C. § 1332(d)(10).

14. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2)(C), because this is a class action in which the amount in controversy exceeds $5,000,000, and at least one member of the class is a citizen of a state other than at least one defendant.

15. This Court has personal jurisdiction over the Defendants because the violations occurred in New York and because defendants L&T and Saks are both headquartered in New York.

16. Venue is appropriate in this District pursuant to 28 USC § 1391(b)(1) because defendants L&T and Saks are headquartered in this District and HBC conducts business in this District.

III. PARTIES

17. Plaintiff Cassondra Joseph ("Plaintiff") is (and was during the period of the Data Breach) a citizen and resident of the State of New York. She shopped at HBC stores—including several Saks and L&T locations—in New York during the period of compromise and purchased merchandise using two different credit cards.

18. Plaintiff has shopped at numerous Saks and L&T locations throughout New York City and elsewhere in upstate New York, and has used two different credit cards to purchase merchandise at these stores. The first card, issued by Chase Bank, has already been used by criminals to make fraudulent charges. Plaintiff has suffered burden, hassle, annoyance, and frustration in disputing these fraudulent charges with Case Bank. Plaintiff's second card has not yet been the subject of any fraudulent charges to Plaintiff's knowledge and Plaintiff must now

expend time and effort to diligently review her statements to determine whether this card too will be subject to fraud.

19. Plaintiff would not have shopped at HBC's stores had Defendants told her that it failed to maintain adequate computer systems and data security practices to safeguard her PII from theft.

20. Plaintiff suffered **actual past injury** from having her PII compromised and/or stolen as a result of the Data Breach, including time spent dealing with fraud resulting from the Data Breach and monitoring her accounts for fraud. Plaintiff also suffered actual past injury in the form of damages to and diminution in the value of her PII.

21. Plaintiff is also at risk of imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her PII being placed in the hands of criminals who have already misused such information stolen in the Data Breach via sale of hers and Class members' PII on the Internet black market.

22. Plaintiff has a continuing interest in ensuring that her private information is protected and safeguarded from future breaches.

23. Plaintiff, who suffered a loss of use of her account funds as a result of the Data Breach, was not reimbursed for the loss of access to or restrictions placed upon her accounts or the resulting loss of use of her own funds.

24. Defendant HBC is a Canadian corporation amalgamated under the Canada Business Corporations Act and domiciled in Canada. The Company owns and operates department stores in Canada and the United States including, among others, Lord & Taylor, Saks Fifth Avenue, and Saks Fifth Avenue OFF 5TH (sometimes "Saks Off 5th" or "Saks Off Fifth").

25. Defendant Saks is a Tennessee corporation registered to do business in New York State and maintains offices in this District at 12 East 49th Street, New York, NY 10017, among other locations.

26. Defendant L&T is a Delaware Domestic Limited Liability Company which is registered in New York State and maintains offices in this District, among other locations.

IV. FACTUAL ALLEGATIONS

27. HBC owns and operates retail stores throughout the United States. For its fiscal year 2017, HBC generated retail sales of CAD$6.682 billion in the United States. As of March 2017, HBC operated more than 470 stores under banners such as the Bay, Saks Fifth Avenue, Lord & Taylor, Gilt, and Saks OFF 5th.

28. In March of 2017, HBC admitted that email addresses and phone numbers of certain Saks Fifth Avenue customers were exposed online over a weekend, and that the exposure was connected to a product wait-list for Saks.com. In response to this first data breach, HBC promised that it would "continually review and enhance security" on its website.

29. This first breach arrived as HBC was struggling to improve its financial performance. In June of 2017 HBC launched a transformation plan to, *inter alia*, cut costs. As part of this transformation plan, HBC chose not to sufficiently invest in the technology to encrypt payment card data at point-of-sale to make its customers' data more secure. Instead, it focused its technology budget on other systems which had more direct impact on the bottom line, despite promising to "enhance security."

30. At the exact same time that HBC was cutting costs, hackers were infiltrating Defendants' payment systems. On April 1, 2018, a data security company called Gemini Advisory reported:

Key Judgements

• On March 28, 2018, a JokerStash hacking syndicate announced the release for sale of over five million stolen credit and debit cards

• In cooperation with several financial organizations, we have confirmed with a high degree of confidence that the compromised records were stolen from customers of Saks Fifth Avenue and Lord & Taylor stores.

• We estimate the window of compromise to be May 2017 to present.

• Based on the analysis of the available data, the entire network of Lord & Taylor and 83 Saks Fifth Avenue locations have been compromised. The majority of stolen credit cards were obtained from New York and New Jersey locations.

• As of this writing, approximately 125,000 records have been released for sale, although we expect the entire cache to become available in the following months.

Executive Summary

On March 28, 2018, a notorious hacking JokerStash syndicate, also known as Fin7 announced the latest breach of yet another major corporation, with more than five million stolen payment cards offered for sale on the dark web. Several large financial institutions have confirmed that all tested records had been used before at Saks Fifth Avenue, Saks Fifth Avenue OFF 5TH, a discounted offset brand of luxury Saks Fifth Avenue stores, as well as Lord & Taylor stores.

Although at this moment it is close to impossible to ascertain the exact window of compromise, the preliminary analysis suggests that criminals were siphoning the information between May 2017 to present. Based on the analysis of the available data, the entire network of Lord & Taylor and 83 Saks Fifth Avenue locations have been compromised. The majority of stolen credit cards were obtained from New York and New Jersey locations.

* * *

With the declared number of compromised payment cards being in excess of five million, the current hacking attack is amongst the biggest and most damaging to ever hit retail companies.

With the declared number of compromised payment cards being in excess of five million, the current hacking attack is amongst the biggest and most damaging to ever hit retail companies.

Using our analytical tools, which were specifically developed in order to empower financial companies to monitor assets portfolio exposure within the deep & dark web, we have established with a high level of confidence that victims of the attack are Saks Fifth Avenue, Saks Fifth Avenue OFF 5TH, a discounted outlet of the luxury department store Saks Fifth Avenue, and Lord & Taylor Stores. Both companies are operated by Canadian retail business group Hudson's Bay Company (HBC). Despite the fact that HBC owns other retail brands, namely Galeria Kaufhof, and Home Outfitters, it appears that only Saks Fifth Avenue and Lord & Taylor were affected in this breach. The company also operates Gilt.com, a popular online shopping website.

As of this writing, only a minor part of compromised records have been offered for sale, with approximately 35,000 records for Saks Fifth Avenue and 90,000 records for Lord & Taylor.

Considering the rather standard practice of marketplace operators in releasing stolen data gradually in order to avoid oversaturation of the market and to minimize the chances of identification of stolen records by the banks, it will take at least several months before the entire archive is offered for sale. For example, in the previous breach of Jason's Deli Restaurants in December of 2017, the JokerStash syndicate has announced that they stole five million payment cards; however, up until now, only approximately a quarter of all payment cards were released for sale.

Despite the fact that the number of stolen records in both breaches is identical, the potential damage to cardholders could be significantly higher in the latest hacking attack. While diners at the affordable fast-food chain are less likely to purchase hi-end electronics like Apple computers and Microsoft Surface Books, which are coveted by cybercriminals for their high liquidity, it is also easier for banks to identify unusual shopping patterns and promptly block out-ofpattern transactions. However, cardholders who frequently shop at luxury retail chains like Saks Fifth Avenue are more likely to purchase high-ticket items regularly; therefore, it will be extremely difficult to distinguish fraudulent transactions from those of a legitimate nature, allowing criminals to abuse stolen payment cards and remain undetected for a longer period of time.

Analysis

Based on the analysis of records that are currently available, it appears that all Lord & Taylor and 83 US based Saks Fifth Avenue locations have been compromised. In addition, we identified three potentially compromised stores located in Ontario, Canada. However, the majority of stolen credit cards were obtained from New York and New Jersey locations.

31. Later that same day (April 1, 2018), The Wall Street Journal reported in an article entitled "Saks, Lord & Taylor Hit With Data Breach; Millions of credit cards exposed by hackers; retailer says it has identified the problem" that:

> Hackers breached the payment systems of Saks Fifth Avenue and Lord & Taylor department stores and stole credit card information for millions of shoppers, the latest in a series of intrusions that have exposed security gaps in corporate networks.
>
> Hackers claim they have five million credit card and debit card numbers from the stores and have been releasing them for sale on the "dark web," a network of websites used by hackers and others to anonymously share information, according to Gemini Advisory LLC, a New York-based cybersecurity firm. The hackers began stealing the card numbers in May 2017, the firm estimates.
>
> A spokesman for Hudson's Bay Co. of Canada, which owns the two chains, confirmed a security breach involving customer payment card data at its Saks Fifth Avenue, Saks Off 5th and Lord & Taylor chains in North America.
>
> He said an investigation is ongoing and didn't say how many accounts were exposed. At this point, the company doesn't believe Social Security or driver's license numbers have been compromised and said it would notify any affected customers once it has completed its investigation.
>
> "We have identified the issue, and have taken steps to contain it," the spokesman said, adding that the company is coordinating with law enforcement. Customers will be offered free identity protection services, including credit monitoring, and won't be liable for fraudulent charges, he said.
>
> The retailer said there was no indication at this time that the breach affected its e-commerce operations, or other store brands it owns, including the Hudson's Bay department-store chain in Canada or Galeria Kaufhof in Germany.
>
> So far, 125,000 cards that had been used at Saks or Lord & Taylor have been released for sale by the hackers, according to Gemini Advisory. Some were cards that were used by card owners as recently as last month in one of the affected stores, according to Dmitry Chorine, Gemini Advisory's chief technology officer.
>
> The group behind the hack is known as JokerStash Syndicate or Fin 7. It appears to have penetrated the retailers' point of sale systems, Mr. Chorine said.
>
> After previous breaches the JokerStash group has released credit card data in smaller batches, to avoid flooding the market for illegally obtained payment credentials, Mr. Chorine said.

The incident is the latest in a string of hacks that have compromised consumer data….

* * *

To make their systems more secure, retailers have been switching to a new form of payment called EMV, for Europay Mastercard and Visa, which uses a computer chip in the card to authenticate transactions.

Hudson's Bay said all Saks Fifth Avenue and Saks Off 5th stores had EMV systems installed by the fall of 2016, while Lord & Taylor stores were equipped with the system by February 2017.

The breach is the latest challenge for Hudson's Bay, which acquired Lord & Taylor in 2012 and Saks in 2013. Like other department store operators, it has been struggling with slowing or declining sales as shoppers buy more online, shift their preferences to specialty stores and spend more of their budgets on travel and entertainment.

In addition, Hudson's Bay has had to contend with an activist investor and a recent CEO switch. In February, the company hired CVS Health Inc. executive Helena Foulkes as chief executive, filling a position that was vacated last fall.

Last week, the company reported mixed results for its latest quarter, with same-store sales rising at Saks but falling at its department store group and off-price division. Ms. Foulkes told analysts that "everything is on the table" when it comes to fixing the business. "There are no sacred cows," she said on a conference call.

For the 12 months ended Feb. 3, the company reported a loss of 581 million Canadian dollars ($450 million) and total sales that were little changed at C$14.4 billion.

32. Also on April 1, 2018, ABC News reported:

A data breach at department store chains Saks Fifth Avenue, Saks Off Fifth and Lord & Taylor has compromised the personal information of customers who shopped at the stores.

The chains' parent company, Canada-based Hudson's Bay Co., announced the breach of its store payment systems on Sunday. The company said it was investigating and taking steps to contain the attack.

The disclosure came after New York-based security firm Gemini Advisory LLC revealed on Sunday that a hacking group known as JokerStash or Fin7 began boasting on dark websites last week that it was putting up for sale up to 5 million

stolen credit and debit cards. The hackers named their stash BIGBADABOOM-2. While the extent of its holdings remains unclear, about 125,000 records were immediately released for sale.

The security firm confirmed with several banks that many of the compromised records came from Saks and Lord & Taylor customers.

Hudson's Bay said in a statement that it "deeply regrets any inconvenience or concern this may cause," but it hasn't said how many Saks or Lord & Taylor stores or customers were affected. The company said there's no indication that the breach affected its online shopping websites or other brands, including the Home Outfitters chain or Hudson's Bay stores in Canada.

The company said customers won't be liable for fraudulent charges. It plans to offer free credit monitoring and other identity protection services.

There is evidence that the breach began about a year ago, said Dmitry Chorine, Gemini Advisory's co-founder and chief technology officer. He said the prolific hacking group has previously targeted major hotel and restaurant chains.

The breach follows last year's high-profile hack of credit bureau Equifax that exposed the personal data of millions of Americans.

This newest breach, however, more closely resembles past retail breaches that have targeted the point-of-sale systems used by companies from Home Depot to Target and Neiman Marcus.

Chorine said the hackers' typical method is to send cleverly crafted phishing emails to company employees, especially managers, supervisors and other key decision-makers. Once an employee clicks on an attachment, which is often made to look like an invoice, the system gets infected. "For an entire year, criminals were able to sit on the network of Lord & Taylor and Saks and steal data," he said. Chorine said most of the stolen credit cards appear to have been obtained from stores in the New York City metropolitan area and other Northeast U.S. states. It's possible, he said, that those stores hadn't yet adopted the more secure credit card payment systems that have been rolled out elsewhere.

Hudson's Bay is advising customers who want more information about the breach to visit security-response websites it's created for Saks Fifth Avenue, Saks Off Fifth, and Lord & Taylor.

33. As of April 2, 2018, substantially identical messages appeared on the three websites identified in the April 1, 2018, Press Release. The substantially identical messages state:

April 2, 2018

Updated Statement

We recently became aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. We identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores. While the investigation is ongoing, there is no indication that this affects our e-commerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe. We deeply regret any inconvenience or concern this may cause.

We wanted to reach out to our customers quickly to assure them that they will not be liable for fraudulent charges that may result from this matter. Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize. We are working rapidly with leading data security investigators to get our customers the information they need, and our investigation is ongoing. We also are coordinating with law enforcement authorities and the payment card companies. For further information, please visit https://www.saksfifthavenue.com/securityinformation/notice.html, https://www.saksoff5th.com/securityinformation/notice.html, or https://www.lordandtaylor.com/securityinformation/notice.html. To speak with a dedicated call center representative, beginning April 4, 2018, you can call 1-855-270-9187, Monday – Saturday, 8 am – 8 pm CT.

FAQs

1. What happened?

We recently became aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. We identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores. While the investigation is ongoing, there is no indication at this time that this affects our ecommerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe. We are working rapidly with leading data security investigators to get our customers the information they need, and our investigation is ongoing. We also are coordinating with law enforcement authorities and the payment card companies.

2. What are you doing about it?

We identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores. We will offer those impacted free identity protection services, including credit and web monitoring.

3. How do I know if my payment card data was affected by this issue?

Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.

4. Will I be liable for fraudulent charges that may result from this matter?

We want to assure our customers that they will not be liable for fraudulent charges that may result from this matter. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize. We will offer those impacted free identity protection services, including credit and web monitoring.

5. Have Social Security or Social Insurance numbers, driver's license numbers, or PINs been affected by this issue?

There is no indication based on our investigation that Social Security or Social Insurance numbers, driver's license numbers, or PINs have been affected by this issue.

6. What should I do now?

It's always a good practice for customers to closely monitor their account statements. If you see an unauthorized charge or a charge you do not recognize, you should notify your card issuer immediately.

7. When will you be able to share more information?

Our investigation is ongoing, and we will do so once we have more clarity around the facts. To speak with a dedicated call center representative, beginning April 4, 2018, you can call 1-855-270-9187, Monday – Saturday, 8 am – 8 pm CT. We will provide additional information to our customers through our websites.

April 1, 2018 Statement

We have become aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in

North America. While the investigation is ongoing, there is no indication at this time that this affects our ecommerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe. We deeply regret any inconvenience or concern this may cause.

We wanted to reach out to our customers quickly to assure them that they will not be liable for fraudulent charges that may result from this matter. We have identified the issue, and have taken steps to contain it. Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.

We are working rapidly with leading data security investigators to get our customers the information they need, and our investigation is ongoing. We also are coordinating with law enforcement authorities and the payment card companies. For further information, please visit https://www.saksfifthavenue.com/securityinformation/notice.html, https://www.saksoff5th.com/securityinformation/notice.html, or https://www.lordandtaylor.com/securityinformation/notice.html. In the coming days, customer care representatives will be available through a dedicated call center to provide further information.

FAQs

1. What happened?

We have become aware of a data security issue involving customer payment card data at certain Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor stores in North America. While the investigation is ongoing, there is no indication at this time that this affects our ecommerce or other digital platforms, Hudson's Bay, Home Outfitters, or HBC Europe. We are working rapidly with leading data security investigators to get our customers the information they need, and our investigation is ongoing. We also are coordinating with law enforcement authorities and the payment card companies.

2. What are you doing about it?

We have identified the issue, and have taken steps to contain it. We will offer those impacted free identity protection services, including credit and web monitoring.

3. How do I know if my payment card data was affected by this issue?

Once we have more clarity around the facts, we will notify our customers quickly and will offer those impacted free identity protection services, including credit and web monitoring. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.

4. Will I be liable for fraudulent charges that may result from this matter?

We want to assure our customers that they will not be liable for fraudulent charges that may result from this matter. We encourage our customers to review their account statements and contact their card issuers immediately if they identify activity or transactions they do not recognize.

We will offer those impacted free identity protection services, including credit and web monitoring.

5. Have Social Security or Social Insurance numbers, driver's license numbers, or PINs been affected by this issue?

There is no indication based on our investigation that Social Security or Social Insurance numbers, driver's license numbers, or PINs have been affected by this issue.

6. What should I do now?

It's always a good practice for customers to closely monitor their account statements. If you see an unauthorized charge or a charge you do not recognize, you should notify your card issuer immediately.

7. When will you be able to share more information?

Our investigation is ongoing, and we will do so once we have more clarity around the facts. To speak with a dedicated call center representative, beginning April 4, 2018, you can call 1-855-270-9187, Monday – Saturday, 8 am – 8 pm CT. We will provide additional information to our customers through our websites.

34. On April 27, 2018, Defendants released an updated statement regarding the Data Breach, stating:

Letter from Our CEO

April 27, 2018

NOTICE OF DATA BREACH

To Our Valued Customers,

As we previously shared, we recently became aware of a data security issue involving customer payment card data at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America. Based on our investigation to date, there is no indication that this issue affects our e-commerce or other digital platforms, or Hudson's Bay, Home Outfitters, or HBC Europe. Our customers are our top priority and we take the protection of their information very seriously. We deeply regret any concern this issue may have caused. Throughout this process, we have made it our goal to work quickly to provide support and information to our customers. We have taken steps, as described below, to address this issue and help protect our customers.

What Happened?

As soon as we became aware of a potential issue, we quickly engaged leading data security experts to conduct an investigation. We also have been working with law enforcement authorities and coordinating with the payment card companies. Based on the investigation to date, we understand that, around July 1, 2017, malware began running on certain point of sale systems at potentially all Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America. We have contained the issue and believe it no longer poses a risk to customers shopping at our stores. Not all customers who shopped at the potentially impacted stores during the relevant time period are affected by this issue. We want to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter.

What Information Was Involved?

The malware was designed to collect customers' payment card information, including cardholder name, payment card number and expiration date. We have no evidence based on the investigation that contact information, Social Security or Social Insurance numbers, driver's license numbers, or PINs associated with the cards were affected by this issue. The investigation has found that this issue did not affect Saks Fifth Avenue credit cards, which are the 9-digit to 14-digit cards that can be used by customers only when shopping at Saks Fifth Avenue or Saks OFF 5TH.

What We Are Doing

As we previously disclosed, we identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores. As indicated

above, we quickly engaged leading data security experts to conduct an investigation. We also have been working with law enforcement authorities and coordinating with the payment card companies. We continue to take steps to enhance the security of our systems and prevent this type of issue from happening again.

What You Can Do

We encourage potentially impacted customers to consider the following data security recommendations:

- Register for Identity Protection Services. We have arranged with AllClear ID to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them. Information about these services is contained in the Reference Guide below and at https://hbc.allclearid.com/.

- Review Your Account Statements. We encourage you to remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your card issuer immediately. We want to reassure our customers that they will not be liable for fraudulent charges that may result from this matter.

- Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you are a Canadian resident, you may order a copy of your credit report from each of the major Canadian credit reporting agencies by contacting Equifax Canada at www.equifax.ca or 1-800-465-7166 or TransUnion Canada at www.transunion.ca, 1-800-663-9980 (English) or 1-877-713-3393 (French).
- Review the Reference Guide. The Reference Guide below provides additional recommendations on the protection of personal information.

For More Information

If you have any questions about this issue, please call 1-855-270-9187, Monday - Saturday, 8 am - 8 pm CT.

We deeply regret any inconvenience or concern this may cause our customers.

Sincerely,

Helena Foulkes
CEO, HBC

April 27, 2018

REFERENCE GUIDE

Potentially impacted customers may take the following steps:

Register for Identity Protection Services. We have arranged with AllClear ID to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them. The following identity protection services start on April 4, 2018, and will be available at any time during the next 12 months.

- AllClear Identity Repair: This service is automatically available to potentially impacted customers with no enrollment required. If a problem arises, customers may receive fraud assistance by calling 1-855-270-9187, Monday - Saturday, 8 am - 8 pm CT, and a dedicated investigator will help them recover financial losses, restore their credit, and return their identity to its proper condition.

- AllClear Fraud Alerts with Credit Monitoring: For U.S. residents, this service includes the ability to set, renew, and remove 90-day fraud alerts on a credit file to help protect against credit fraud. In addition, this offering includes credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, customers will need to provide certain information to AllClear ID. Potentially impacted customers may sign up online at https://hbc.allclearid.com/ or by calling 1-855-270-9187.

- AllClear Identity Theft Monitoring Canada: For Canadian residents, this service offers additional layers of protection, including identity theft monitoring that delivers actionable alerts by phone. To enroll in this service, customers will need to provide certain information to AllClear ID. Potentially impacted customers may sign up by calling 1-855-270-9187 or by emailing global@allclearid.com.

- TransUnion Canada Credit Monitoring: For Canadian residents, this service is available through TransUnion of Canada, Inc. ("TransUnion") and includes 12 months of credit monitoring and credit file access. Customers who enroll in this service will receive fraud-watch emails that will alert them when changes are made to their credit file, such as new credit-related inquiries, new accounts, late payments and more. To request a TransUnion Canada Credit Monitoring code, potentially impacted customers may call 1-855-270-9187 or email global@allclearid.com.

Please note: Additional steps may also be required to activate the monitoring options.

***

HBC: Updated Website FAQs

1. What happened?

As we previously shared, we recently became aware of a data security issue involving customer payment card data at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America. As soon as we became aware of a potential issue, we quickly engaged leading data security experts to conduct an investigation. We also have been working with law enforcement authorities and coordinating with the payment card companies. Based on the investigation, we understand that, around July 1, 2017, malware began running on certain point of sale systems at potentially all Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America. There is no indication based on our investigation that this affects our e-commerce or other digital platforms, or Hudson's Bay, Home Outfitters, or HBC Europe. We have contained the issue and believe it no longer poses a risk to customers shopping at our stores. Not all customers who shopped at the potentially impacted stores during the relevant time period are affected by this issue.

2. What information was affected by this issue?

The malware was designed to collect customers' payment card information, including cardholder name, payment card number and expiration date. We have no evidence based on the investigation that contact information, Social Security or Social Insurance numbers, driver's license numbers, or PINs associated with payment cards were affected by this issue. The investigation has found that this issue did not affect Saks Fifth Avenue credit cards, which are the 9-digit to 14-digit cards that can be used by customers only when shopping at Saks Fifth Avenue or Saks OFF 5TH.

3. How do I know if my payment card data was affected by this issue?

While we do not know if your specific payment card is affected by this issue, we encourage potentially impacted customers to refer to their payment card statements to identify the payment card they may have used at Saks Fifth Avenue, Saks OFF 5TH or Lord & Taylor locations in North America from July 1, 2017 through March 31, 2018. Not all customers who shopped at the potentially impacted stores during the relevant time period are affected by this issue. If you believe there is an unauthorized charge on your card, please contact the card issuer immediately. We want to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter. It is always a good idea to be checking your statements regularly.

The investigation has found that this issue did not affect Saks Fifth Avenue credit cards, which are the 9-digit to 14-digit cards that can be used by customers only when shopping at Saks Fifth Avenue or Saks OFF 5TH. In addition, there is no indication that this issue affects payment cards used on our e-commerce or other digital platforms.

4. Is it safe to use a payment card at our stores?

We identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores.

5. What are you doing to assist potentially impacted customers?

We have arranged with AllClear ID to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them. Information about these services is contained in the Reference Guide above and at https://hbc.allclearid.com/.

6. Will I be liable for fraudulent charges that may result from this matter?

We want to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter. We encourage you to review your account statements and contact your card issuer immediately if you identify an unauthorized charge on your card. We have arranged to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them.

7. What should I do to help protect my information?

We encourage you to review your account statements and contact your card issuer immediately if you identify an unauthorized charge on your card. We want to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter.

If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to review your account statements and monitor your free credit reports. For more information about steps you can take to protect your credit files, you can contact any one of the consumer reporting agencies at:

Equifax	1-800-525-6285	www.equifax.com
Experian	1-888-397-3742	www.experian.com
TransUnion	1-800-680-7289	www.transunion.com

If you are a Canadian resident, you may order a copy of your credit report from each of the major Canadian credit reporting agencies by contacting Equifax Canada at www.equifax.ca or 1-800-465-7166 or TransUnion Canada at www.transunion.ca, 1-800-663-9980 (English) or 1-877-713-3393 (French).

8. How do I find out more about the identity protection services?

We have arranged to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them. Information about these services is contained in the Reference Guide above and at https://hbc.allclearid.com/. If you have any questions about this issue, please call 1-855-270-9187, Monday - Saturday, 8 am - 8 pm CT.

9. Where can I get more information?

If you have any questions about this issue, please call 1-855-270-9187, Monday - Saturday, 8 am - 8 pm CT.

April 27, 2018 Statement

HBC Provides Update on Previously-Announced Data Security Issue at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor Locations in North America

NEW YORK & TORONTO--(April 27, 2018)--HBC (TSX:HBC) today provided an update on its investigation into the previously-disclosed data security issue involving customer payment card data at Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America.
HBC contained the issue on March 31, 2018 and believes it no longer poses a risk to customers shopping at its stores. The company wants to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter.

HBC CEO Helena Foulkes said, “Our customers are our top priority and we take the protection of their information very seriously. We deeply regret any concern this issue may have caused. Throughout this process, we have made it our goal to work quickly to provide support and information to our customers and we will continue to serve them with that same dedication.”

As soon as HBC became aware of a potential issue, the company quickly engaged leading data security experts to conduct an investigation. HBC also has been working with law enforcement authorities to address this criminal activity and has been coordinating with the payment card companies. Based on the investigation to date, the company has determined the following:

Around July 1, 2017, malware began running on certain point of sale systems at potentially all Saks Fifth Avenue, Saks OFF 5TH and Lord & Taylor locations in North America.

- Not all customers who shopped at the potentially impacted stores during the relevant time period are affected by this issue.

- There is no indication that this issue affects the company's e-commerce or other digital platforms, or Hudson's Bay, Home Outfitters, or HBC Europe.

- The malware was designed to collect customers' payment card information, including cardholder name, payment card number and expiration date. The company has no evidence that contact information, Social Security or Social Insurance numbers, driver's license numbers, or PINs associated with the cards were affected by this issue.

- The investigation has found that this issue did not affect Saks Fifth Avenue credit cards, which are the 9-digit to 14-digit cards that can be used by customers only when shopping at Saks Fifth Avenue or Saks OFF 5TH.

HBC has arranged to provide potentially impacted customers with identity protection services, including credit and web monitoring, at no cost to them. Those customers can register for identity protection services at https://hbc.allclearid.com/. HBC encourages customers to review their account statements and contact their card issuer immediately if they identify an unauthorized charge on their card.

HBC has put in place a dedicated call center for customers to obtain more information about this matter. Customers with questions may call 1-855-270-9187, Monday through Saturday, 8:00 am to 8:00 pm CT. Updated information regarding this issue has been posted at https://www.saksfifthavenue.com/security-information/notice.html, https://www.saksoff5th.com/security-information/notice.html, and https://www.lordandtaylor.com/security-information/notice.html.

HBC directs investors to its public filings available at www.sedar.com and at www.hbc.com for additional information and risk factors.

35. In discussing security, L&T's Privacy Policy, updated as of the July 17, 2017, stated:

We maintain certain physical, administrative, and technical steps to safeguard the information we collect from and about our customers and Site visitors. While we make every effort to help ensure the integrity and security of our network and systems, we cannot guarantee our security measures. When you enter alternative

> information (such aa credit card information) on our forms, we encrypt the transmission of that information using secure socket layer technology (SSL).

36. In discussing security, Saks's Privacy Policy and Website Terms of Use, updated as of the February 10, 2014, stated:

> Protecting the security of your information is very important to us. When you transmit sensitive personal information (such as credit card information) from your computer to our servers, your information is protected by both a "firewall" (a combination of computer hardware and software that helps keep unauthorized visitors from accessing information within our computer network) and industry standard SSL (secure socket layer) encryption. For our mobile website, we protect your payment card information using encryption technology when you place an order. Once we receive your transmission, we will take reasonable precautions to secure and protect the Information on our systems. Unfortunately, no data transmission over the Internet can be 100% secure and, accordingly, we cannot guarantee or warrant the security of any information you disclose or transmit to us online. However, we strive to protect your information and privacy.

37. HBC indicated in its Press Releases that it will offer free identity protection services, including credit and web monitoring. This form of credit monitoring is of reduced value because it is reactionary—it is not designed to prevent fraud, but merely to monitor it. It also does not address past harm suffered by Plaintiff

38. Plaintiff and members of the Class defined below have or will suffer actual injury as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims—including Plaintiff—spent or will spend substantial time and expense relating to:

a. Uncovering fraudulent charges;

b. Canceling and requesting cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

39. As a direct and proximate result of HBC's conduct, Plaintiff and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiff now must expend time and effort to mitigate the actual and potential impact of the Data Breach, including placing "freezes" and "alerts" with credit reporting agencies, contacting her financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Moreover, Plaintiff and the Class have an interest in ensuring that their information, which remains in the possession of HBC, is protected from any additional breaches by the implementation of security measures and safeguards.

40. Plaintiff and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury directly flowing from potential fraud and identity theft related to customers' PII being up for sale on the Internet black market;

d. Damages flowing from HBC's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' PII for which there is a well-established and quantifiable national and international market; and

h. The loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

V. CLASS ACTION ALLEGATIONS

41. Plaintiff bring this class action pursuant to Federal Rule of Civil Procedure 23 on behalf of a nationwide class defined as follows:

> All residents of the United States whose personal information was compromised as a result of the data breach first disclosed by HBC on April 1, 2018.

42. Excluded from the Class are Defendants, their past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns, and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

43. Numerosity: the Class Members are so numerous and dispersed nationwide that joinder of all members is impractical. Upon information and belief, the number exceeds several million, although the exact number is unknown.

44. Commonality: common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. These common questions include the following, among others:

a. Whether Defendants committed the actions alleged herein;

b. Whether Defendants had a legal duty to adequately protect Plaintiff's and the Class' PII;

c. Whether Defendants breached their duty by failing to adequately protect Plaintiff's and the Class' PII;

d. Whether Defendants had a legal duty to provide to Plaintiff and the Class timely time and accurate notice of the Data Breach;

e. Whether Defendants breached their duty to provide timely time and accurate notice of the Data Breach;

f. Whether and when Defendants knew or should have known that Plaintiff's and the Class' PII stored on their computer systems was vulnerable or susceptible to theft;

g. Whether and when Defendants knew or should have known that Plaintiff's and the Class' PII stored on their computer systems was compromised;

h. Whether Defendants have an implied contractual obligation to use reasonable data security measures to safeguard and protect Plaintiff's and the Class' PII;

i. Whether Defendants breached any implied contractual obligation to use reasonable data security measures;

j. Whether Defendant's actions were materially deceptive or misleading;

k. Whether Defendant's actions occurred within the State of New York and within the United States of America;

l. Whether the Class Members are "consumers" within the meaning of New York's consumer protection statute;

m. Whether Plaintiff and the Class are entitled to recover actual/statutory damages; and

n. Whether Plaintiff and the Class are entitled to equitable relief, including an injunction.

45. Typicality: Plaintiff's claims are typical of the claims of all other Class Members. Plaintiff and Class members were injured through HBC's uniform misconduct and their legal claims arise from the same core practices.

46. Adequacy: Plaintiff will fairly and adequately protect the interests of all members of the Class in the prosecution of this action. Plaintiff is similarly situated with, and has similar injuries to, the members of the Class she seeks to represent. Plaintiff is an adult and has retained counsel experienced in complex class action matters generally and in the emerging fields of digital privacy and data breach litigation, specifically.

47. Superiority: A class action is superior to all other available methods for the fair and efficient adjudication of this case because joinder of all members is impractical if not impossible. Furthermore, the cost of litigating each claim individually might exceed actual and/or statutory damages available to each class member thus making it impossible for each class member to litigate his or her claims individually. There will be no difficulty in managing this action as a class action.

VI. COUNTS

COUNT I
Violation of New York' Consumer Protection Statute
(General Business Law § 349)

48. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

49. New York General Business Law § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state . . . ."

50. Defendants' acts, including making representations to consumers that it possessed sufficient data security to safeguard Plaintiff's and the Class' PII, were intended to induce and did induce, Plaintiff and the Class to provide their PII to Defendants.

51. Defendants engaged in material, deceptive, consumer-oriented acts in the conduct of its business in this state, as alleged herein, including by:

a. Actively and knowingly misrepresenting or omitting material information to Plaintiff and the Class at the time they provided their PII, including that Defendants did not have sufficient data security to protect the PII;

b. Failing to give adequate warning and notice regarding defects and problems with Defendants' systems used to protect Plaintiff's and the Class' PII. Defendants knew or should have known of the inherent defects in its data security systems and failed to address these defects or to provide adequate and timely notice that there had been a Breach.

52. Defendants' conduct is and was deceptive, false, and fraudulent, and constitutes an unconscionable commercial practice in that Defendants have, through the use of false or

deceptive statements and/or knowing and intentional material omissions, misrepresented and/or concealed their defective data security system and failed to timely and adequately reveal the Data Breach.

53. Plaintiff and the Class were deceived by and relied upon Defendants' affirmative misrepresentations and omissions.

54. Such acts by Defendants are deceptive acts or practices are material and mislead reasonable consumers into providing their PII to Defendants. Requests for and use of Plaintiff's and the Class' PII materials in New York and concerning New York residents and/or citizens was a consumer-oriented act.

55. Defendants' wrongful conduct caused Plaintiff and the Class to suffer consumer-related injury by causing them to incur substantial expense to protect from misuse of their PII by third parties and placing Plaintiff and the Class at serious risk of monetary damages.

56. As a direct and proximate result of Defendant's violation of § 349, Plaintiff and the Class have suffered actual damages in an amount to be determined at trial.

57. Defendant willfully and/or knowingly violated § 349(a).

58. Section 349(h) provides a private right of action to enforce § 349(a) to recover each Plaintiff's actual damages or $50 statutory damages per Class Member, whichever is greater.

59. Section 349(h) authorizes the Court to increase the amount not to exceed three times actual damages up to $1,000 per Class Member if the Court finds that Defendant willfully or knowingly violated this section.

60. Section 349(h) also authorizes the Court to award attorney's fees to a prevailing Plaintiff in addition to damages.

COUNT II
Negligence

61. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

62. Defendants invited Plaintiff and the Class into their stores, and ultimately solicited, gathered, and stored Plaintiff's and the Class PII to, *inter alia*, facilitate sales transactions there.

63. Defendants knew or should have known of the risks inherent in collecting and storing Plaintiff's and the Class' PII and the importance of adequate data security. Defendants received warnings from within and outside the company that hackers routinely attempted to access PII. Defendants also knew about numerous, well-publicized data breaches of other national retailers and restaurant chains.

64. Defendants owed duties of care to Plaintiff and the Class whose PII was entrusted to them. Defendants' duties included:

a. Exercising reasonable care in handling PII;

b. Safeguarding Plaintiff's and the Class' PII using reasonable and adequate security procedures and systems consistent with industry-standard practices;

c. Implementing processes to quickly detect a data breach and to timely act on warnings about breaches; and

d. Promptly notifying Plaintiff and the Class of any data breach.

65. Because Defendants knew that the Data Breach would damage Plaintiff and the Class, Defendants had a duty to adequately protect the PII.

66. Defendants owed a duty of care not to subject Plaintiff and the Class to an unreasonable risk of harm because such risks were foreseeable and probable to victims of any actor with inadequate data security practices.

67. Defendants knew, or should have known, that their computer systems did not adequately safeguard Plaintiff's and the Class' PII.

68. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class' PII.

69. Defendants breached their duties of care by failing to provide prompt notice of the Data Breach to Plaintiff and the Class whose PII was compromised. To date, Defendants have not provided sufficient information regarding the extent and scope of the Data Breach and continues to breach its disclosure obligations.

70. Defendants acted with reckless disregard for the security of Plaintiff's and the Class' PII because Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII that that they collected and stored, which hackers were attempting to access.

71. Defendants acted with reckless disregard for Plaintiff's and the Class' rights by failing to provide prompt and adequate notice of the Breach so that they could take measures to protect themselves from damages caused by the fraudulent use of their compromised PII.

72. Defendants had a special relationship with Plaintiff and the Class. Plaintiff's and the Class' willingness to entrust Defendants with their PII was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their data systems (and the PII stored therein).

73. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class. Defendants' misconduct included failing to:

a. Secure its point-of-sale systems;

b. Secure access to its servers;

c. Comply with industry standard data security practices;

d. Encrypt PII at the point-of-sale and during transit;

e. Employ adequate network segmentation;

f. Implement adequate system and event monitoring;

g. Utilize modern payment systems that provided significantly more data security against intrusion;

h. Install updates and patches in a timely manner; and

i. Implement the systems, policies, and procedures necessary to prevent this type of Data Breach.

74. Defendants also had independent duties under state laws that required them to reasonably safeguard Plaintiff's and the Class' PII and promptly notify them of any data breach.

75. Defendants breached their duties owed to Plaintiff and the Class in numerous ways, including by:

a. Creating a foreseeable risk of harm through the misconduct described herein;

b. Failing to implement adequate security systems, protocols, and practices sufficient to protect their PII both before and after learning of the Data Breach;

c. Failing to comply with the minimum industry data security standards; and

d. Failing to timely and accurately disclose that Plaintiff's and the Class' PII had been improperly acquired or accessed.

76. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and the Class, their PII either would not have been compromised or they would have been able to prevent some or all of their damages.

77. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and the Class have suffered damages.

78. The injury and harm that Plaintiff and the Class suffered (as alleged above) was reasonably foreseeable.

79. Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract

80. Plaintiff realleges, as if fully set forth, the allegations of the preceding paragraphs.

81. Defendants invited customers, including Plaintiff and the Class, to make purchases at their stores use payment cards in order to increase sales by making purchases more convenient. Plaintiff and the Class accepted Defendants' offers and made purchases at Defendants' stores.

82. When Plaintiff and Class provided their PII to Defendants in making purchases at Defendants' stores, they entered into implied contracts by which Defendants agreed to protect their PII and timely notify them in the event of a data breach.

83. An implicit part of the offer was that Defendants would safeguard the PII using reasonable or industry-standard means and would timely notify Plaintiff and the Class in the event of any data breach. Each purchase was made pursuant to this mutually agreed upon implied contract.

84. Defendants also affirmatively represented that it would "continually review and enhance security" after a prior data leak.

85. Based on the implicit understanding and also on Defendants' representation, Plaintiff and the Class accepted the offers and provided Defendants with their PII by using payment cards in connection with purchases at Defendants' locations during the period of the Data Breach.

86. Plaintiff and the Class would not have provided and entrusted their PII to Defendants had they known that Defendants would not safeguard their PII as promised or provide timely notice of any data breach.

87. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

88. Defendants breached the implied contracts by failing to safeguard Plaintiff's and the Class' PII and failing to provide them with timely and accurate notice when their PII was compromised in the Data Breach.

89. The losses and damages Plaintiff and the Class sustained were the direct and proximate result of Defendants' breaches of their implied contracts with Plaintiff and the Class.

COUNT IV
Unjust Enrichment

90. Plaintiff incorporate the above allegations by reference as if set forth fully herein.

91. Plaintiff and the Class conferred monetary benefit on Defendants. Plaintiff and the Class made purchases and paid for goods sold by Defendants, and provided Defendants with PII for the purchases that they would not have otherwise made had they known that Defendants did not provide adequate protection for their PII. In exchange for these purchases and payment, Plaintiff and the Class bargained adequate data security for their PII.

92. Defendants knew that Plaintiff and the Class conferred a benefit on Defendants. Defendants profited from purchases and used customers' PII for their own business purposes.

93. The payments made for goods sold by Defendants should have been used by Defendants, at least in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

94. Defendants failed to properly secure Plaintiff's and the Class' PII and was thus unjustly enriched by not providing the full benefit of the bargain made with Plaintiff and the Class.

95. As a result of Defendants' conduct described herein, Plaintiff and the Class suffered actual damages.

96. If Plaintiff and the Class were aware of Defendants' failure to safeguard their PII, they would not have shopped with them.

97. Plaintiff and the Class have no adequate remedy at law.

98. Under these circumstances and principles of equity and good conscience, it is unjust for Defendants to retain the benefits that Plaintiff and the Class conferred upon them because Defendants failed to use that money to implement the reasonable data privacy and security practices and procedures that Plaintiff and the Class paid for.

99. Defendants should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiff and the Class proceeds that they unjustly received.

100. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and the Class overpaid.

COUNT V
Declaratory Judgement, 28 U.S.C. § 2201

101. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

102. An actual controversy, over which this Court has jurisdiction, has arising and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendants for which Plaintiff desires a declaration of rights.

103. Plaintiff contends that Defendants' acts, practices, and conduct constitute a breach of contract and violate state law.

104. Plaintiff and the Class entered into an implied contract that required Defendants to provide adequate security for the PII it collected from their transactions.

105. Defendants owe duties of care to Plaintiff and the Class.

106. Defendants still possess PII regarding Plaintiff and the Class.

107. Since the Data Breach, Defendants have announced no changes to their data security to address the vulnerabilities which permitted the intrusions.

108. Defendants have not yet satisfied their contractual obligations and legal duties to Plaintiff and the Class.

109. The Data Breach has caused actual harm regarding Defendants contractual obligations and duties of care to provide security measures to Plaintiff and the Class. Additionally, Plaintiff and the Class are at risk of additional or further harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

110. There is no reason to believe that Defendants' security measures are any more adequate than they were prior to the Data Breach to meet Defendants' contractual obligations and legal duties, and there is no reason to believe Defendants have no other security vulnerabilities that have not yet been knowingly exploited.

111. Plaintiff therefore seeks a declaration (1) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate

security, and (2) that Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on their systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such security auditors;

b. ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants data systems is compromised hackers cannot gain access to other portions of the systems;

e. ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

f. ordering that Defendants conduct regular database scanning and securing checks;

g. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when one occurs and what to do in response to a breach; and

h. ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Certify this action as a Class Action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoints Plaintiff as class representative and her counsel as Class Counsel;

B. Award compensatory damages, including statutory damages, to Plaintiff and the Class for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiff and the Class against Defendants;

D. Award punitive damages in an amount that will deter Defendants and others from like conduct;

E. Permanently restrain Defendants and their officers, agents, employees, and attorneys from violating the statutes referred to herein;

F. Award Plaintiff reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

G. Grant Plaintiff such further relief as the Court deems appropriate.

VIII. JURY DEMAND

Plaintiff demands a trial by jury of all issues triable.

Dated: May 23, 2018
New York, NY

KAPLAN FOX & KILSHEIMER LLP

/s/ David Straite

David A. Straite
Ralph E. Labaton
850 Third Avenue
New York, NY 10022
dstraite@kaplanfox.com
Tel.: 212.687.1980
Fax: 212.687.7714

-and-

Laurence D. King
350 Sansome Street, Suite 400
San Francisco, CA 94104
Tel: 415.772.4700
Fax: 415.772.4707